대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2001년 제 81105 호
Application Number PATENT-2001-0081105

출 원 년 월 일 : 2001년 12월 19일
Date of Application DEC 19, 2001

출 원 인 : 한국전자통신연구원
Applicant(s) KOREA ELECTRONICS & TELECOMMUNICATIONS RESEARCH INS

2002 년 01 월 08 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【참조번호】 0004

【제출일자】 2001.12.19

【발명의 명칭】 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법

【발명의 영문명칭】 METHOD OF DESIGNING PASSWORD BASED AUTHENTICATION AND KEY EXCHANGE PROTOCOL USING ZERO-KNOWLEDGE INTERACTIVE PROOF

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【성명】 권태복

【대리인코드】 9-2001-000347-1

【포괄위임등록번호】 2001-057650-1

【대리인】

【성명】 이화익

【대리인코드】 9-1998-000417-9

【포괄위임등록번호】 1999-021997-1

【발명자】

【성명의 국문표기】 양대헌

【성명의 영문표기】 NYANG,Dae-Hun

【주민등록번호】 701028-1140816

【우편번호】 405-234

【주소】 인천광역시 남동구 간석4동 579-1 23/2

【국적】 KR

【발명자】

【성명의 국문표기】 이석준

【성명의 영문표기】 LEE,Sok-Joon

【주민등록번호】 760126-1400611

【우편번호】 302-739
【주소】 대전광역시 서구 만년동 상아아파트 106동 306호
【국적】 KR
【발명자】
【성명의 국문표기】 정병호
【성명의 영문표기】 CHUNG,Byung-Ho
【주민등록번호】 640208-1558710
【우편번호】 302-754
【주소】 대전광역시 서구 월평3동 진달래아파트 110동 105호
【국적】 KR
【공지예외적용대상증명서류의 내용】
【공개형태】 1. 학술단체 서면발표
【공개일자】 2001.06.24
【심사청구】 청구
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인
권태복 (인) 대리인
이화익 (인)
【수수료】
【기본출원료】 20 면 29,000 원
【가산출원료】 6 면 6,000 원
【우선권주장료】 0 건 0 원
【심사청구료】 13 항 525,000 원
【합계】 560,000 원
【감면사유】 정부출연연구기관
【감면후 수수료】 280,000 원
【첨부서류】 1. 요약서·명세서(도면)_1통 2.공지예외적용대상(신규성상실의예외, 출원시의특례)규정을 적용받 기 위한 증명서류_1통

【요약서】

【요약】

본 발명은 대화형 영 지식 증명을 이용하여 패스워드 기반의 인증 및 키 교환을 안전하게 수행하는 프로토콜의 설계 방법에 관한 것이다. 본 방법에서는, 먼저, 인증에 필요한 각종 시스템 파라미터를 설정한다. 그리고, 그 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수를 선택하여, 사용자 ID, 소정의 일방향 함수를 적용한 시험수(A), 및 서버와 사용자에게만 알려지는 질문수를 생성하기 위한 값(X)으로 이루어진 메시지를 서버에게 보낸다. 그 후, 이 메시지를 이용하여 서버가 서버의 공개키 소유 여부에 대한 증명(Auth)과 서버와 사용자에게만 알려지는 질문수를 생성하기 위한 값(Y)으로 이루어진 메시지를 사용자에게 보낸다. 사용자가 그 Auth를 검증해서 서버를 인증하고, 서버와 사용자만 아는 비밀 동전 던지기의 결과 값(c)과 세션 키(SK)를 계산 후, 사용자 인증을 위해 목격자 수(B)를 서버에게 전송한다. 그 후, 각 사용자에 대한 패스워드 확인자(V)가 보관된 서버가 c를 이용하여 그 B를 검증하고, SK를 계산하여 세션 키를 교환한다. 따라서, 본 발명은, 대화형 영 지식 증명 프로토콜을 사용하면서도 스마트카드 등의 도구없이 패스워드만 기억하므로써 안전한 인증 및 키교환을 할 수 있도록 도와준다.

【대표도】

도 1

【색인어】

인증 프로토콜, 대화형 영 지식 증명, 패스워드, 사용자 인증, 키 교환

【명세서】

【발명의 명칭】

대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법{METHOD OF DESIGNING PASSWORD BASED AUTHENTICATION AND KEY EXCHANGE PROTOCOL USING ZERO-KNOWLEDGE INTERACTIVE PROOF}

【도면의 간단한 설명】

도 1은 본 발명의 사용자 인증 과정 및 키 교환 알고리즘의 프레임웍을 나타낸 도면,

도 2는 본 발명의 사용자 인증 과정 및 키 교환 프레임웍에 RSA 문제를 적용한 프로토콜을 나타낸 도면,

도 3은 본 발명의 사용자 인증 과정 및 키 교환 프레임웍에 이산 대수 문제를 적용한 프로토콜을 나타낸 도면,

도 4는 본 발명의 사용자 인증 과정 및 키 교환 프레임웍에 소인수 분해에 기초한 제곱근 문제를 적용한 프로토콜을 나타낸 도면.

도면의 주요 부분에 대한 부호의 설명

50 : 사용자 60 : 서버

100 : 시스템 설정

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<8> 본 발명은 통신망에서 패스워드를 이용해서 사용자 인증 및 안전한 통신을 위한 키 교환을 수행하기 위한 방법에 관한 것으로, 특히 기존의 대화형 영 지식 증명(Zero-Knowledge Interactive Proof)을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법에 관한 것이다. 이러한 사용자는 다른 일체의 도구 없이 패스워드만을 기억함으로써 자신의 신분을 증명할 수 있고, 이후의 통신에 사용될 세션 키를 안전하게 서버와 공유할 수 있게 된다. 여기서, 사용자는 인증 요청을 수행하는 주체이고, 서버는 인증을 수행하는 주체를 나타낸다.

<9> 상기와 같이 패스워드를 이용한 사용자 인증은, 통신에 참여하는 두 주체가 상대방이 자신이 통신하려고 하는 그 주체임을 패스워드를 통해 확인하는 과정을 말한다. 이때, 사용자 인증에 필요한 정보 이외에 아무런 정보도 상대방에게 노출해서는 안된다. 또한, 패스워드를 이용한 키 교환은, 통신에 참여하는 두 주체가 키를 공유하는 과정을 말한다. 이때, 도청자가 이 공유된 키를 알 수 없도록 해야한다.

<10> 또한, 패스워드는 대칭키 또는 공개키 암호 시스템 등에서 사용되는 키와는 달리, 매우 짧고 랜덤성도 크지 않으므로 패스워드를 이용한 사용자 인증 및 키 교환 프로토콜은 오프라인 사전 공격에 공격당하기 쉽다.

<11> 일반적인 영 지식 증명이 사용자 인증에 사용되기는 하지만 키로서 패스워드를 사용하는 경우에는 안전하지 못하다. 그러나, 본 발명에서는 일반적인 영 지식 증명 프로토콜이, 키로서 패스워드를 갖는 경우에도 안전하게 수행 될 수 있는 방법을 제시한다.

<12> 현재 사용되고 있는 패스워드를 이용한 인증 프로토콜은 오프라인 사전 공격(offline dictionary attack)에 매우 취약한 것으로 알려져 있다. 이를 보완하기 위해서 Tom Wu의 SRP, David Jablon의 B-SPEKE, Belloving 등의 EKE 등이 설계되었다. 하지만 기존의 사용자 인증 프로토콜은 패스워드를 이용하는 경우 그 안전성이 수학적으로 증명되지 않았다. 최근에는 EKE(encrypted key exchange)의 일부분에 대해 안전성이 증명되었으며, 수학적인 안전성 증명을 갖는 프로토콜들이 제안되었으나 대부분 adhoc 설계에 의존하고 있다.

<13> 또한, 인증 프로토콜중 패스워드를 이용하지 않고 공개키 암호시스템을 사용하는 경우 사용자의 비밀키나 인증서를 저장하고 있는 스마트카드 등의 보안 토큰을 사용자가 소지해야하는 불편함이 따른다. 따라서, 종래기술에 의하면, 패스워드를 이용한 인증 및 키 교환 프로토콜의 편리함을 제공하지 못한다.

【발명이 이루고자 하는 기술적 과제】

<14> 따라서, 상기와 같은 문제점을 해결하기 위해서, 본 발명은, 오프라인 사전 공격에 대해 수학적인 안전성 증명을 가지며, adhoc 설계가 아닌 체계적인 패스워드 기반 인증 프로토콜 설계를 가능하게 하는데 하나의 목적이 있다.

<15> 또한, 본 발명은, 본 발명에서 정의하는 패스워드 기반의 인증 및 키 교환 프로토콜을 이용할 경우 사용자로 하여금 패스워드만을 기억하게 함으로써, 사용자 자신을 인증시킬 수 있고, 키 교환을 수행할 수 있게 하는데 다른 목적이 있다.

<16> 부연하면, 본 발명은, 주어진 대화형 영 지식 증명을 이용해서 패스워드 기반의 인증 및 키 교환 프로토콜을 체계적으로 설계하는 방법을 제공한다. 이러한 본 발명은, 어떤 영 지식 증명이 주어졌을 때 새로운 인증 및 키 교환 프로토콜로 변환 할 수 있는 방법이다.

【발명의 구성 및 작용】

<17> 상술한 목적을 달성하기 위해 본 발명의 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법을 제공한다. 이 방법은, 먼저, 인증에 필요한 각종 시스템 파라미터를 설정한다. 그 후, 그 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r, x)를 선택하여, 사용자 ID(IDuser), 일방향 함수(OWF)를 적용해서 얻은 시험수인 (A=OWF(r)), 및 서버와 사용자에게만 알려지는 제 1 질문수 생성 값(X)으로 이루어진 메시지를 서버에게 보낸다. 이 보내진 메시지를 이용하여 서버가 서버의 공개키 소유 여부에 대한 증명(Auth)과 서버와 사용자에게만 알려지는 제 2 질문수 생성 값(Y)으로 이루어진 메시지를 사용자에게 보낸다. 사용자가 상기 Auth를 검증해서 서버를 인증하고, 서버와 사용자만 아는 비밀 동전 던지기의 결과 값(c)과 세션 키(SK)를 계산한다. 이와 같이 서버와 사용자만 아는 비밀 동전 던지기의 결과 값으로 인해 오프라

인 사전공격을 막을 수 있다. 그 계산 후, 사용자 인증을 위해 목격자 수(B)를 서버에게 전송한다. 각 사용자에 대한 패스워드 확인자(V=OWF(f(P))가 비밀리에 보관된 서버가 목격자 수(B)를 상기 A, V 및 c를 이용해 검증하고, SK를 계산하여 세션 키를 교환한다. 이에 따라서, 본 발명에서 주어진 대화형 영 지식 증명을 이용해서 패스워드 기반의 인증 및 키 교환 프로토콜을 체계적으로 설계할 수 있다.

<18> 또한, 본 발명에서는, 도 1의 프레임웍에 RSA 문제, 이산 대수 문제 및 소인수 분해 문제에 대응한 패스워드 확인자가 각각 서버에 비밀리에 보관되고, 상기 문제에 대응하게 사용자가 목격자 수(B)를 서로 다르게 하고, 이러한 서로 다른 목격자 수에 상응하게 검증요소를 다르게 한다. 이들은, 이후에 상세히 설명하겠다.

<19> 이와 같이 본 발명은, 종래기술에서처럼 하나의 인증 프로토콜만을 제시하지 않고, 암호학에 대한 깊은 지식 없이도 쉽게 새로운 인증 및 키 교환 프로토콜을 설계할 수 있는 방법을 여러 문제에 상응하게 응용할 수 있다.

<20> 이하, 사용자가 패스워드만을 이용해서 자신을 서버에게 인증시키고 이후의 안전한 통신을 위해 키를 교환하는 본 발명의 실시예들을 첨부된 도면을 참조하여 설명하겠다.

<21> 도 1은 패스워드를 이용한 인증 및 키 교환 프로토콜의 프레임웍을 도시한 것이다.

<22> 먼저, 사용자(50)와 서버(60)가 프로토콜을 수행하기 전에 시스템 파라미터를 미리 설정해 둔다(100). 시스템 파라미터는 사용자와 서버간의 약속으로, 시스템 전체를 통해 사용자들이 공유하게 된다. G는 배수 그룹(multiplicative group) Z^*_p나 타원 곡선그룹 등의 유한 순환 그룹이고, g는 유한 순환 그룹 G의 생성기(generator)이다. 본 발명에서는 편의상 배수 그룹 표기법을 따랐다. OWF는 일방향 함수(oneway function)로서, 본 발명의 실시예들에서는, RSA(Rivest, Shamir, Adleman) 문제에 기초한 일방향 함수, 이산 대수 문제에 기초한 일방향 함수 또는 소인수 분해 문제에 기초한 일방향 함수 등으로 한정되어 예시되었지만, 이외의 다른 문제에 기초한 일방향 함수의 예에서도 본 발명이 적용 가능하다. 그리고, f(P)는 패스워드 P를 OWF의 입력값이 되도록 길이를 늘려주는 함수이고, 암호학적 성질을 가질 필요는 없다. V(x)는 x를 키 V로 대칭키 암호화하는 것, $V^{-1}(x)$는 x를 키 V로 대칭키 복호화하는 것을 의미한다. 여기서, 대칭키 암호는 잘 알려진 DES, 3DES, RC5, AES 등이 될 수 있다. H()는 sha-1, md5 등의 해쉬함수이고, ||는 연결(concatenation)을 의미한다.

<23> 도 1에서 사용자의 비밀 정보는 패스워드뿐이고, 서버의 비밀 정보는 각 사용자에 대한 패스워드 확인자 V=OWF(f(P))가 된다.

<24> 도 1에서 사용자(50)는 사용자 ID(ID_{User}), 랜덤수 r을 임의로 선택해서 계산한(101a) 시험수 A=OWF(r), 및 랜덤수 x를 임의로 선택해서 계산한(101b) 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $X=V(g^x)$를 포함한 메시지를 서버(60)에게 전송한다(101). 이에 따라, 사용자 및 서버의 인증과, 키 교환 프로토콜을 시작할 수 있게 된다.

<25> 상기 전송된 메시지를 받은 서버(60)는, 그 메시지를 이용하여 랜덤수 y를 임의로 선택하여 계산한 서버의 공개키 소유여부에 대한 증명 Auth=H(K'||1)(102a)과 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $Y=V(g^y)$(102b)를 포함한 메시지를 사용자(50)에게 전송한다(102). 위에서, Auth=H(K'||1)는 $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$를 이용해서 계산한다. 이 과정에 따라서, 다음 과정에서 사용자가 서버 인증정보 및 랜덤 도전(random challenge)(도면부호 103b에서 'c')을 계산하도록 해준다.

<26> 서버(60)로부터 전송된(102) 메시지를 받은 사용자(50)는 다음식, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$을 계산해서 Auth를 검증한다. 이 검증결과, 성공하면 서버(60)가 패스워드 확인자 V를 알고 있음을 사용자(50)는 확신할 수 있다. 그러므로, 사용자는 서버의 패스워드 확인자 소유여부를 확인함으로써 서버 인증을 완료할 수 있다(103a). 그리고, 사용자(50)는, 상기 A와 TSK=H(K'||0)를 이용해 c=H(TSK||A)를 계산한다. 이때, c는 비밀 동전 던지기의 결과가 되며, 일반적인 영 지식 증명에서 c는 평문형태로 서버에서 사용자로 전송되는 것과는 달리 서버와 사용자만 아는 c값이다. 또한, 이와 같이 인증을 수행하는 주체인 서버가 인증 요청을 수행하는 주체인 사용자에게 인증을 위해 전송하는 랜덤 도전(상기 c를 말함)을 서버와 사용자만 알도록 함으로써 오프라인 사전 공격을 막을 수 있다. 이와 마찬가지로, 후술하는 도 2, 도 3 및 도 4에서도 서버와 사용자만이 랜덤 도전을 알도록 함으로써 오프라인 사전 공격을 막을 수 있다.

<27> 이와 같이 계산 후, 사용자는 목격자 수 B를 상술한 c, r 그리고 자신이 가지고 있는 패스워드 P를 이용해서 계산한 후 서버에게 전송한다(103b). 아울러, 사용자는, 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(103c). 상기 세 진행 단계 103a 내지 103c로 이루어져, 사용자가 서버를 인증하고, 목격자 수 B를 전송하는 과정(103)을 수행한다.

<28> 서버(60)는 c=H(TSK||A)를 계산하고 사용자의 목격자수 B를 A, V, c를 이용해서 검증한다. 그 검증 결과, 성공하면 서버의 사용자 인증이 완료된다(104a). 그리고, 서버는 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(104b). 이 프로토콜 종료 후, 사용자와 서버 사이에 교환된 세션키는 SK=H(K'||A||B||2)이다(104).

<29> 도 2는 상술한 도 1의 프레임웍에 RSA 문제를 적용한 프로토콜이다. 도 1에서 설명한 시스템 설정과 모두 같은 의미를 갖고, 다른 부분인 (n=p*q, e)은 RSA 공개키이다. 이때, p, q는 RSA 소수이고, e는 소수이다. 따라서 일방향 함수 $OWF(r)=r^e \bmod n$ 이다. f(P)는 패스워드 P를 lg(n) bits로 늘려주는 함수이다(200).

<30> 도 2에서 사용자의 비밀 정보는 패스워드뿐이고, 서버의 비밀 정보는 각 사용자에 대한 패스워드 확인자 $V=[f(P)^{-1}]^e \bmod n$가 된다.

<31> 도 2에서 사용자(50)는 사용자 ID(ID_{User}), 랜덤수 r을 임의로 선택해서 계산한(201a) 시험수 $A=r^e \bmod n$, 및 랜덤수 x를 임의로 선택해서 계산한(201b) 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $X=V(g^x)$를 포함한 메시지를 서버(60)에게 전송한다(201).

<32> 상기 전송된 메시지를 받은 서버(60)는, 그 메시지를 이용하여 랜덤수 y를 임의로 선택하여 계산한 서버의 공개키 소유여부에 대한 증명 Auth=H(K'||1)(202a)과 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $Y=V(g^y)$(202b)를 포함한 메시지를 사용자(50)에게 전송한다(202). 위에서, Auth=H(K'||1)는 $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$ 를 이용해서 계산한다.

<33> 서버(60)로부터 전송된(202) 메시지를 받은 사용자(50)는 다음식, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$을 계산해서 Auth를 검증한다. 이 검증결과, 성공하면 서버(60)가 패스워드 확인자 V를 알고 있음을 사용자(50)는 확신할 수 있다. 그러므로, 사용자는 서버의 패스워드 확인자 소유여부를 확인함으로써 서버 인증을 완료할 수 있다(203a). 그리고, 사용자(50)는, 상기 A와 TSK=H(K'||0)를 이용해 c=H(TSK||A)를 계산한다. 이때, c는 비밀 동전 던지기의 결과가 되며, 일반적인 영 지식 증명에서 c는 평문형태로 서버에서 사용자로 전송되는 것과는 달리 서버와 사용자만 아는 c값이다. 이와 같이 계산 후, 사용자는 목격자 수 B를 상술한 c, r 그리고 자신이 가지고 있는 패스워드 P를 이용해서 계산 후 서버에게 전송한다(203b). 이때의 목격자 수 B는, $B=r*f(P)^c \bmod n$이다. 아울러, 사용자는, 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(203c). 상기 세 진행 단계 203a 내지 203c로 이루어져, 사용자가 서버를 인증하고, 목격자 수 B를 전송하는 과정(203)을 수행한다.

<34> 서버(60)는 c=H(TSK||A)를 계산하고 사용자의 목격자수 B를 $B^e*V^c=A \bmod n$을 이용해서 검증한다. 그 검증 결과, 성공하면 서버의 사용자 인증이 완료된다

(204a). 그리고, 서버는 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(204b). 이 프로토콜 종료 후, 사용자와 서버 사이에 교환된 세션키는 SK=H(K'||A||B||2)이다(204).

<35> 도 3은 상술한 도 1의 프레임웍에 이산대수문제(Discrete Logarithm Problem)를 적용한 프로토콜이다. 도 1에서 설명한 시스템 설정과 모두 같은 의미를 가지며, p는 p-1이 큰 소수 q를 인수로 갖는 소수이다. a는 Z^*_q의 생성기이고, 따라서 OWF(r)=a^r mod p 이다. f(P)는 패스워드 P를 lg(q) bits로 늘려주는 함수이다(300).

<36> 도 3에서 사용자의 비밀 정보는 패스워드뿐이고, 서버의 비밀 정보는 각 사용자에 대한 패스워드 확인자 V=$a^{-f(P)}$ mod p가 된다.

<37> 도 3에서 사용자(50)는 사용자 ID(ID_{User}), 랜덤수 r을 임의로 선택해서 계산한(301a) 시험수 A= a^r mod p, 및 랜덤수 x를 임의로 선택해서 계산한(301b) 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 X=V(g^x)를 포함한 메시지를 서버(60)에게 전송한다(301).

<38> 상기 전송된 메시지를 받은 서버(60)는, 그 메시지를 이용하여 랜덤수 y를 임의로 선택하여 계산한 서버의 공개키 소유여부에 대한 증명 Auth=H(K'||1)(302a)과 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 Y=V(g^y)(302b)를 포함한 메시지를 사용자(50)에게 전송한다(302). 위에서, Auth=H(K'||1)는 K=[$V^{-1}(X)$]^y, K'=H(K||g^x||g^y||ID_{User}||ID_{Server}) 를 이용해서 계산한다.

<39> 서버(60)로부터 전송된(302) 메시지를 받은 사용자(50)는 다음식, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$을 계산해서 Auth를 검증한다. 이 검증 결과, 성공하면 서버(60)가 패스워드 확인자 V를 알고 있음을 사용자(50)는 확신할 수 있다. 그러므로, 사용자는 서버의 패스워드 확인자 소유여부를 확인함으로써 서버 인증을 완료할 수 있다(303a). 그리고, 사용자(50)는, 상기 A와 $TSK=H(K'||0)$를 이용해 $c=H(TSK||A)$를 계산한다. 이때, c는 비밀 동전 던지기의 결과가 되며, 일반적인 영 지식 증명에서 c는 평문형태로 서버에서 사용자로 전송되는 것과는 달리 서버와 사용자만 아는 c값이다. 이와 같이 계산 후, 사용자는 목격자 수 B를 상술한 c, r 그리고 자신이 가지고 있는 패스워드 P를 이용해서 계산 후 서버에게 전송한다(303b). 이때의 목격자 수 B는, $B=r+f(P)*c \bmod q$ 이다. 아울러, 사용자는, 세션 키 SK를 $SK=H(K'||A||B||2)$에 의해 계산한다(303c). 상기 세 진행 단계 303a 내지 303c로 이루어져, 사용자가 서버를 인증하고, 목격자 수 B를 전송하는 과정(303)을 수행한다.

<40> 서버(60)는 $c=H(TSK||A)$를 계산하고 사용자의 목격자수 B를 $a^B*V^c=A \bmod p$를 이용해서 검증한다. 그 검증 결과, 성공하면 서버의 사용자 인증이 완료된다(304a). 그리고, 서버는 세션 키 SK를 $SK=H(K'||A||B||2)$에 의해 계산한다(304b). 이 프로토콜 종료 후, 사용자와 서버 사이에 교환된 세션키는 $SK=H(K'||A||B||2)$이다(304).

<41> 도 4는 상술한 도 1의 프레임웍에 소인수 분해에 기초한 제곱근 문제를 적용한 프로토콜이다. 도 1에서 설명한 시스템 설정과 모두 같은 의미를 가지며,

(n= p*q)는 RSA 공개키이다. 따라서 OWF(r) = r^2 mod n 이다. f(P)는 패스워드 P를 lg(n) bits로 늘려주는 함수이다(400).

<42> 도 4에서 사용자의 비밀 정보는 패스워드뿐이고, 서버의 비밀 정보는 각 사용자에 대한 패스워드 확인자,

<43> $[V_1=[f(P+1)^{-1}]^2 \bmod n,\ V_2=[f(P+2)^{-1}]^2 \bmod n,\ V_3=[f(P+3)^{-1}]^2 \bmod n,\ \ldots,\ V_k=[f(P+k)^{-1}]^2 \bmod n,\ V=H(V_1,V_2,\ldots,V_k)]$가 된다.

<44> 도 4에서 사용자(50)는 사용자 ID(ID_{User}), 랜덤수 r을 임의로 선택해서 계산한(401a) 시험수 A= r^2 mod n, 및 랜덤수 x를 임의로 선택해서 계산한(401b) 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $X=V(g^x)$를 포함한 메시지를 서버(60)에게 전송한다(401).

<45> 상기 전송된 메시지를 받은 서버(60)는, 그 메시지를 이용하여 랜덤수 y를 임의로 선택하여 계산한 서버의 공개키 소유여부에 대한 증명 Auth=H(K'||1)(402a)과 서버와 사용자에게만 알려지는 질문수 생성을 위한 값인 $Y=V(g^y)$(402b)를 포함한 메시지를 사용자(50)에게 전송한다(402). 위에서, Auth=H(K'||1)는 $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$ 를 이용해서 계산한다.

<46> 서버(60)로부터 전송된(402) 메시지를 받은 사용자(50)는 다음식, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$을 계산해서 Auth를 검증한다. 이 검증결과, 성공하면 서버(60)가 패스워드 확인자 V를 알고 있음을 사용자(50)는 확신할 수 있다. 그러므로, 사용자는 서버의 패스워드 확인자 소유여부를 확인함으로

써 서버 인증을 완료할 수 있다(403a). 그리고, 사용자(50)는, 상기 A와 TSK=H(K'||0)를 이용해 c=H(TSK||A)를 계산한다. 이때, c는 비밀 동전 던지기의 결과가 되며, 일반적인 영 지식 증명에서 c는 평문형태로 서버에서 사용자로 전송되는 것과는 달리 서버와 사용자만 아는 c값이다. 이와 같이 계산 후, 사용자는 목격자 수 B를 상술한 c, r 그리고 자신이 가지고 있는 패스워드 P를 이용해서 계산 후 서버에게 전송한다(403b). 이때의 목격자 수 B는,

<47> $$B = r * \prod_{i=1,k} f(P+i)^{c_i}$$

<48> 이다. 아울러, 사용자는, 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(403c). 이렇게 하여서, 사용자가 서버를 인증하고, 목격자 수 B를 전송하는 과정(403)을 수행한다.

<49> 서버(60)는 c=H(TSK||A)를 계산하고 사용자의 목격자수 B를,

<50> $$A = B^2 * \prod V_i^{c_i} \bmod n$$

<51> 를 이용해서 검증한다. 그 검증 결과, 성공하면 서버의 사용자 인증이 완료된다(404a). 그리고, 서버는 세션 키 SK를 SK=H(K'||A||B||2)에 의해 계산한다(404b). 이 프로토콜 종료 후, 사용자와 서버 사이에 교환된 세션키는 SK=H(K'||A||B||2)이다(404).

【발명의 효과】

<52> 이상과 같은 본 발명은 다음과 같은 효과를 갖는다.

<53> 먼저, 본 발명에 의해 설계된 프로토콜은 오프라인 사전 공격(Offline dictionary attack)에 강하다.

<54> 또한, 통신망에서 사용되는 사용자 인증 및 키 교환 프로토콜에 응용될 수 있다. 예를 들어, 인터넷 정보보호를 위해 사용되는 TLS(Transport Layer Security)(IETF(Internet Engineering Task Force)에서 제정한 트랜스포트 계층의 보안 프로토콜)를 인증서와 비밀키 없이 패스워드만으로 수행하도록 정의할 수 있다. 또한, IEEE 802.11i 그룹에서 논의되고 있는 인증프로토콜에 본 발명을 응용할 수도 있다.

<55> 또한, UNIX의 사용자 인증 과정을 본 발명으로 대체할 수도 있다.

<56> 이렇게 본 발명을 실제로 응용하는 것 이외에도, 본 발명에서 제시한 프레임웍을 이용하여 새로운 인증 및 키 교환 프로토콜을 쉽게 설계할 수 있다. 따라서, 사용자가 암호학에 대한 깊은 지식 없이도, 쉽게 안전한 인증 및 키 교환 프로토콜을 설계할 수 있게 된다.

【특허청구범위】

【청구항 1】

인증에 필요한 각 종 시스템 파라미터를 설정하는 제 1 과정과,

상기 설정된 파라미터에 의거하여 사용자가 임의로 랜덤 수(r, x)를 선택하여, 사용자 ID, 일방향 함수를 적용한 시험수(A=OWF(r)), 및 서버와 사용자에게만 알려지는 제 1 질문수 생성 값(X)으로 이루어진 메시지를 서버에게 보내는 제 2 과정과;

상기 메시지를 이용하여 서버가 서버의 공개키 소유 여부에 대한 증명(Auth)과 서버와 사용자에게만 알려지는 제 2 질문수 생성 값(Y)으로 이루어진 메시지를 사용자에게 보내는 제 3 과정과,

사용자가 상기 Auth를 검증해서 서버를 인증하고, 일반적인 영 지식 증명에서 서버와 사용자만 아는 비밀 동전 던지기의 결과 값(c)과 세션 키(SK)를 계산 후, 사용자 인증을 위해 목격자 수(B)를 서버에게 전송하는 제 4 과정과,

각 사용자에 대한 패스워드 확인자(V=OWF(f(P))가 보관된 서버가 상기 B를 상기 A, V 및 c를 이용해 검증하고, SK를 계산하여 세션 키를 교환하는 제 5 과정을 포함하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법.

【청구항 2】

제 1 항에 있어서,

상기 목격자 수(B)는 상기 c, r 및 자신의 패스워드(P)를 이용하여 서버에게 전송하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법.

【청구항 3】

제 1 항에 있어서,

상기 서버의 패스워드 확인자 소유 여부를 사용자가 확인하여 서버를 인증하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법.

【청구항 4】

제 1 항에 있어서,

상기 일방향 함수가 RSA 문제에 기초한 경우 상기 패스워드 확인자를 $V=[f(P)^{-1}]^e \bmod n$ 로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, (n=p*q(p, q는 RSA소수), e(소수))는 RSA 공개키이고, f(P)는 패스워드 P를 lg(n)bit로 늘려주는 함수임).

【청구항 5】

제 1 항 또는 제 4 항에 있어서,

상기 목격자 수(B)를 $B=r*f(P)^c \bmod n$ 으로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, H( )는 해쉬함수임).

【청구항 6】

제 5 항에 있어서,

상기 목격자 수(B)의 검증을 $B^eV^c=A \bmod n$ 을 이용하여 수행하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$.

【청구항 7】

제 1 항에 있어서,

상기 일방향 함수가 이산 대수 문제에 기초한 경우 상기 패스워드 확인자를 $V=a^{-F(p)} \bmod p$ 로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, a는 Z^*_q의 생성기, p는 소수, f(P)는 패스워드 P를 lg(n)bit로 늘려주는 함수임).

【청구항 8】

제 1 항 또는 제 7 항에 있어서,

상기 목격자 수(B)를 $B=r+f(P)*c \bmod q$ 로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, $H(\ )$는 해쉬함수임).

【청구항 9】

제 8 항에 있어서,

상기 목격자 수(B)의 검증을 $a^B V^c=A \bmod p$ 을 이용하여 수행하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, $c=H(TSK||A)$, $TSK=H(K'||0)$, $K=[V^{-1}(Y)]^x$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$.

【청구항 10】

제 1 항에 있어서,

상기 일방향 함수가 소인수 분해 문제에 기초한 경우 상기 패스워드 확인자를 $[V_1=[f(P+1)^{-1}]^2 \bmod n$, $V_2=[f(P+2)^{-1}]^2 \bmod n$, $V_3=[f(P+3)^{-1}]^2 \bmod n$, ..., $V_k=[f(P+k)^{-1}]^2 \bmod n$, $V=H(V_1,V_2, \ldots,V_k)]$로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여

기서, n=p*q(p, q는 RSA 소수), f(P)는 패스워드 P를 lg(n)bit로 늘려주는 함수임).

【청구항 11】

제 1 항 또는 제 10 항에 있어서,

상기 목격자 수(B)를

$$B = r * \prod_{i=1,k} f(P+i)^{c_i}$$

으로 하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, c=H(TSK||A), TSK=H(K'||O), $K=[V^{-1}(X)]^y$, $K'=H(K||g^x||g^y||ID_{User}||ID_{Server}$, 여기서, H( )는 해쉬함수임).

【청구항 12】

제 11 항에 있어서,

상기 목격자 수(B)의 검증을

$$A = B^2 * \prod V_i^{c_i} \bmod n$$

을 이용하여 수행하는 것을 특징으로 하는 대화형 영 지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법(여기서, c=H(TSK||A),

TSK=H(K'||0), K=[$V^{-1}(Y)$]^{x}, K'=H(K||g^{x}||g^{y}||ID_{User}||ID_{Server}, c_i는 c의 i번째 비트임).

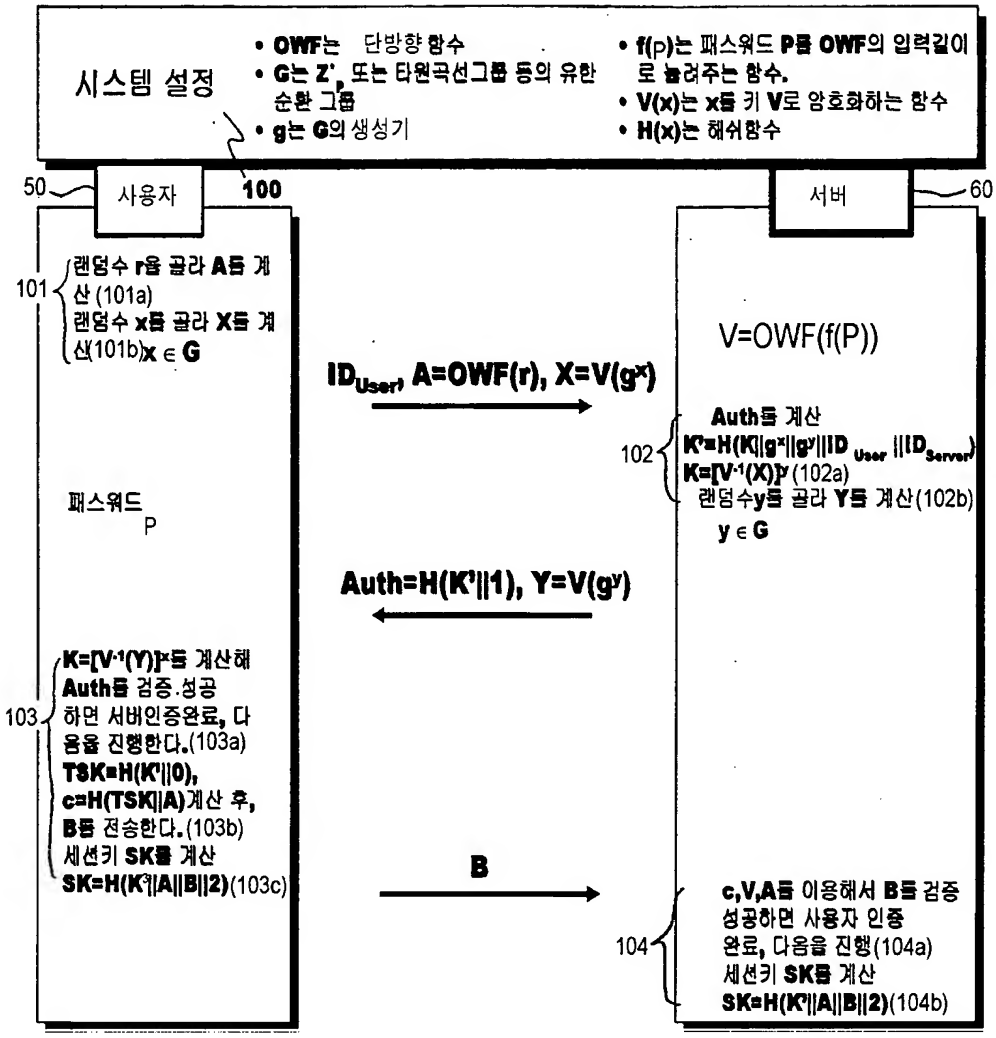
【청구항 13】

제 1 항에 있어서,

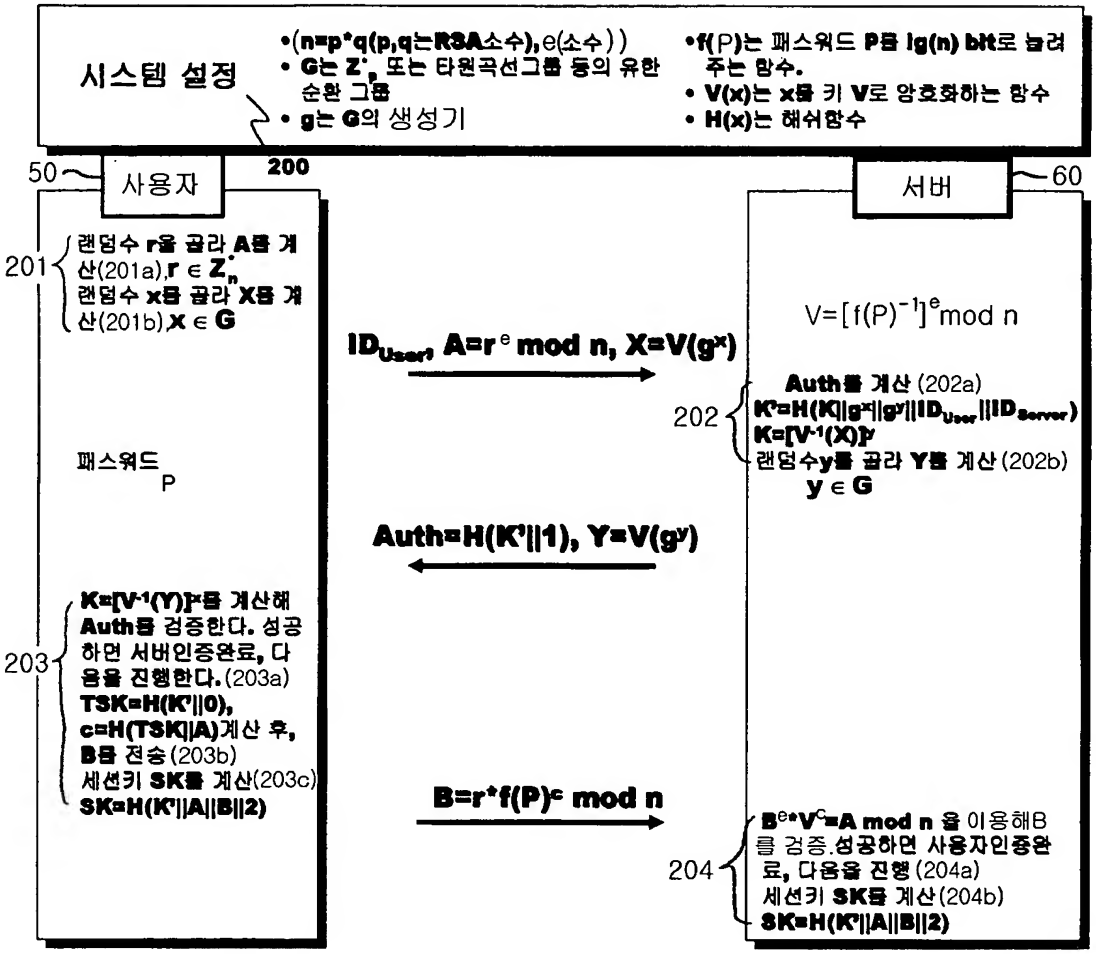
상기 서버가 사용자에게 인증을 위해 전송하는 랜덤 도전을 서버와 사용자만이 알도록 함으로써 오프라인 사전공격을 막는 것을 특징으로 하는 대화형 영지식 증명을 이용한 패스워드 기반의 인증 및 키 교환 프로토콜 설계 방법.

【도면】

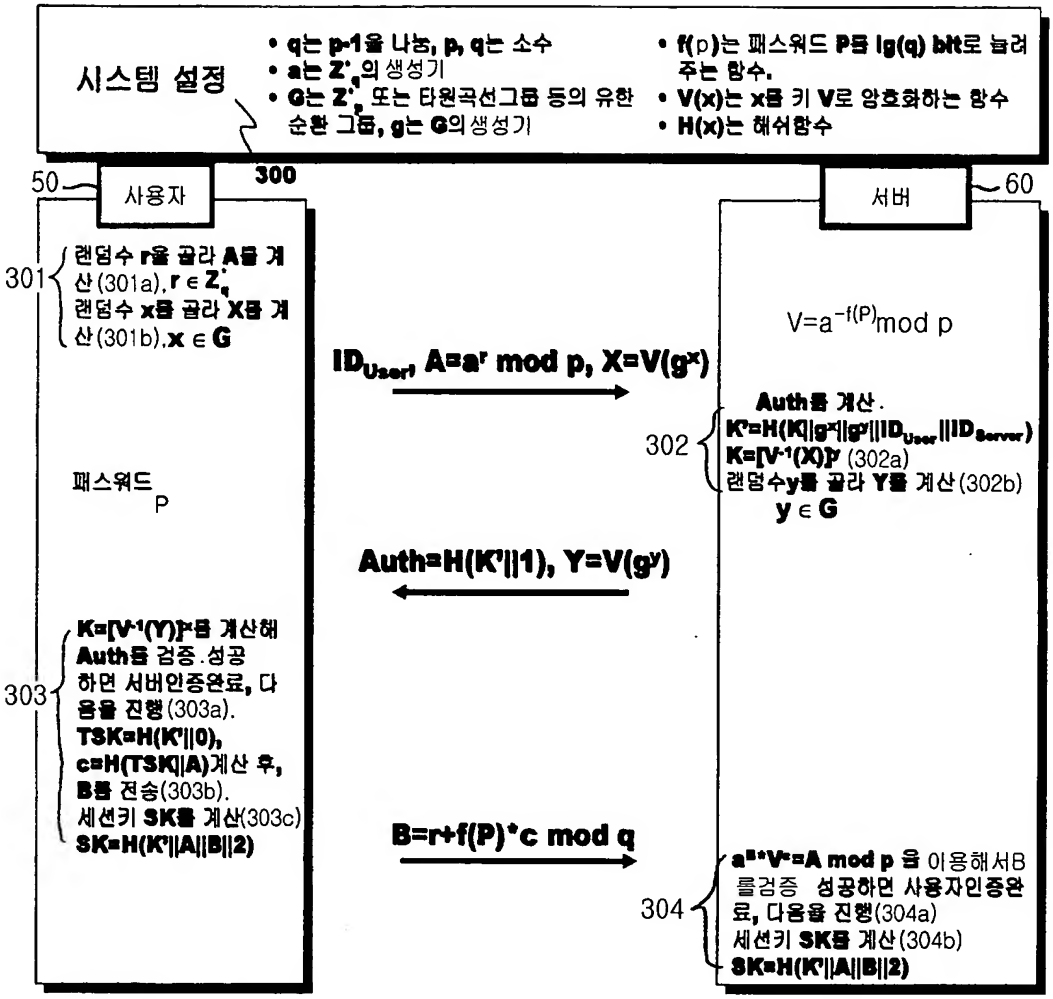
【도 1】


시스템 설정
• OWF는 단방향 함수
• G는 Z*p 또는 타원곡선그룹 등의 유한 순환 그룹
• g는 G의 생성기
• f(p)는 패스워드 P를 OWF의 입력길이로 늘려주는 함수.
• V(x)는 x를 키 V로 암호화하는 함수
• H(x)는 해쉬함수
50
사용자
100
서버
60
101
랜덤수 r을 골라 A를 계산 (101a)
랜덤수 x를 골라 X를 계산(101b)x ∈ G
패스워드 P
V=OWF(f(P))
ID_User, A=OWF(r), X=V(g^x)
102
Auth를 계산
K'=H(K||g^x||g^y||ID_User||ID_Server)
K=[V^-1(X)]^y (102a)
랜덤수y를 골라 Y를 계산(102b)
y ∈ G
Auth=H(K'||1), Y=V(g^y)
103
K=[V^-1(Y)]^x를 계산해 Auth를 검증.성공하면 서버인증완료, 다음을 진행한다.(103a)
TSK=H(K'||0), c=H(TSK||A)계산 후, B를 전송한다.(103b)
세션키 SK를 계산
SK=H(K'||A||B||2)(103c)
B
104
c,V,A를 이용해서 B를 검증 성공하면 사용자 인증 완료, 다음을 진행(104a)
세션키 SK를 계산
SK=H(K'||A||B||2)(104b)

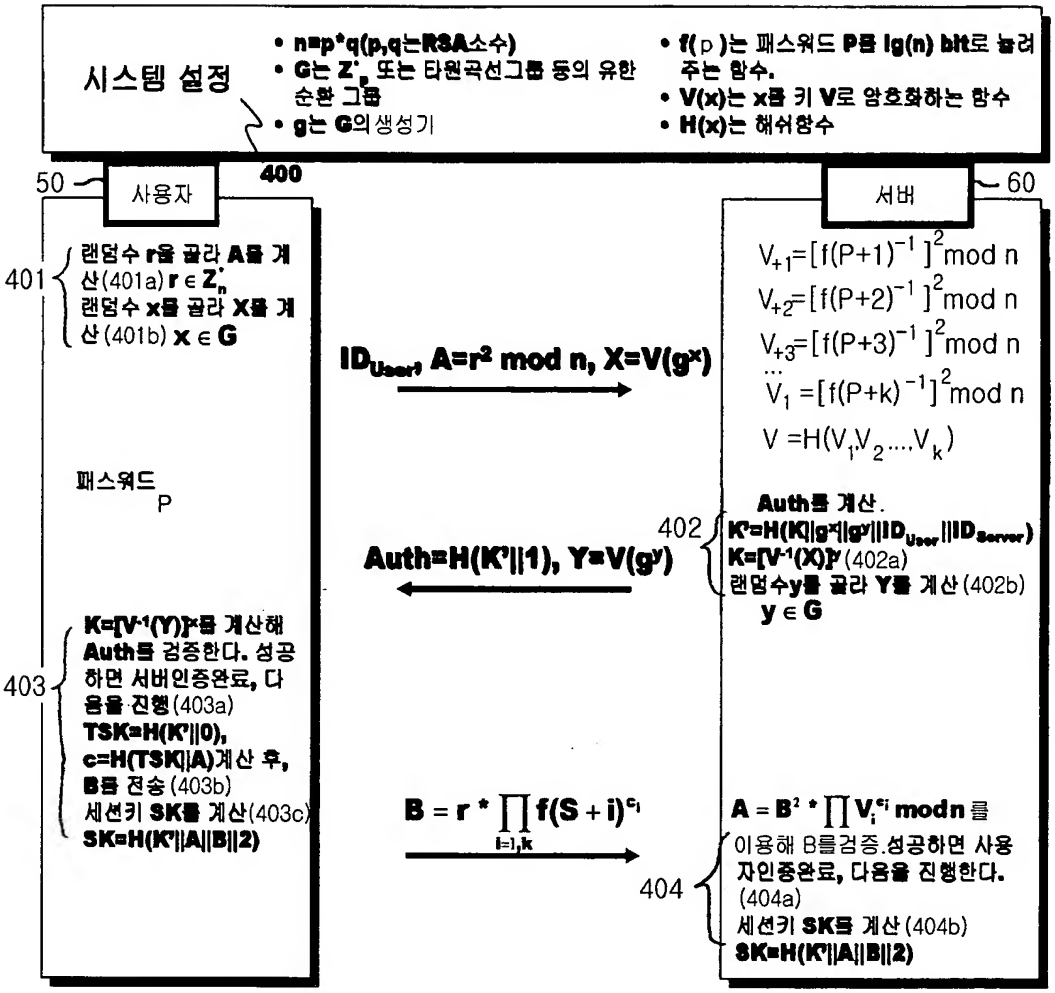
【도 2】


시스템 설정
•(n=p*q(p,q는RSA소수),e(소수))
• G는 Z*n, 또는 타원곡선그룹 등의 유한 순환 그룹
• g는 G의 생성기
•f(P)는 패스워드 P를 lg(n) bit로 늘려 주는 함수.
• V(x)는 x를 키 V로 암호화하는 함수
• H(x)는 해쉬함수
200
50
사용자
서버
60
201
랜덤수 r을 골라 A를 계산(201a), r ∈ Z*n
랜덤수 x를 골라 X를 계산(201b), X ∈ G
패스워드 P
V=[f(P)^-1]^e mod n
ID_User, A=r^e mod n, X=V(g^x)
202
Auth를 계산 (202a)
K'=H(K||g^x||g^y||ID_User||ID_Server)
K=[V^-1(X)]^y
랜덤수y를 골라 Y를 계산 (202b)
y ∈ G
Auth=H(K'||1), Y=V(g^y)
203
K=[V^-1(Y)]^r를 계산해 Auth를 검증한다. 성공하면 서버인증완료, 다음을 진행한다.(203a)
TSK=H(K'||0), c=H(TSK||A)계산 후, B를 전송(203b)
세션키 SK를 계산(203c)
SK=H(K'||A||B||2)
B=r*f(P)^c mod n
204
B^e*V^c=A mod n 을 이용해B를 검증.성공하면 사용자인증완료, 다음을 진행(204a)
세션키 SK를 계산(204b)
SK=H(K'||A||B||2)

【도 3】


시스템 설정
• q는 p-1을 나눔, p, q는 소수
• a는 Z^*_q의생성기
• G는 Z^*_p 또는 타원곡선그룹 등의 유한 순환 그룹, g는 G의생성기
• f(p)는 패스워드 P를 lg(q) bit로 늘려 주는 함수.
• V(x)는 x를 키 V로 암호화하는 함수
• H(x)는 해쉬함수
300
50
사용자
서버
60
301
랜덤수 r을 골라 A를 계산(301a), $r \in Z^*_q$
랜덤수 x를 골라 X를 계산(301b), $x \in G$
$V=a^{-f(P)} \bmod p$
$ID_{User}, A=a^r \bmod p, X=V(g^x)$
302
Auth를 계산.
$K'=H(K||g^x||g^y||ID_{User}||ID_{Server})$
$K=[V^{-1}(X)]^y$ (302a)
랜덤수y를 골라 Y를 계산(302b)
$y \in G$
패스워드 P
$Auth=H(K'||1), Y=V(g^y)$
303
$K=[V^{-1}(Y)]^r$를 계산해 Auth를 검증.성공하면 서버인증완료, 다음을 진행(303a).
$TSK=H(K'||0)$,
$c=H(TSK||A)$계산 후, B를 전송(303b).
세션키 SK를 계산(303c)
$SK=H(K'||A||B||2)$
$B=r+f(P)*c \bmod q$
304
$a^B*V^c=A \bmod p$ 을 이용해서B를검증 성공하면 사용자인증완료, 다음을 진행(304a)
세션키 SK를 계산(304b)
$SK=H(K'||A||B||2)$

【도 4】


시스템 설정
• n=p*q(p,q는RSA소수)
• G는 Z*n 또는 타원곡선그룹 등의 유한 순환 그룹
• g는 G의생성기
• f(p)는 패스워드 P를 lg(n) bit로 늘려 주는 함수.
• V(x)는 x를 키 V로 암호화하는 함수
• H(x)는 해쉬함수
400
50
사용자
서버
60
401
랜덤수 r을 골라 A를 계산(401a) r ∈ Z*n
랜덤수 x를 골라 X를 계산(401b) x ∈ G
ID_User, A=r² mod n, X=V(g^x)
V+1=[f(P+1)^-1]² mod n
V+2=[f(P+2)^-1]² mod n
V+3=[f(P+3)^-1]² mod n
...
V1=[f(P+k)^-1]² mod n
V=H(V1,V2....,Vk)
패스워드 P
402
Auth를 계산.
K'=H(K||g^x||g^y||ID_User||ID_Server)
K=[V^-1(X)]^y (402a)
랜덤수y를 골라 Y를 계산(402b) y ∈ G
Auth=H(K'||1), Y=V(g^y)
403
K=[V^-1(Y)]^x를 계산해 Auth를 검증한다. 성공하면 서버인증완료, 다음을 진행(403a)
TSK=H(K'||0), c=H(TSK||A)계산 후, B를 전송(403b)
세션키 SK를 계산(403c)
SK=H(K'||A||B||2)
B = r * ∏ f(S+i)^ci (i=1,k)
404
A = B² * ∏ Vi^ci mod n를 이용해 B를검증.성공하면 사용자인증완료, 다음을 진행한다. (404a)
세션키 SK를 계산(404b)
SK=H(K'||A||B||2)